BLANKROME

Cybersecurity & Data Privacy

APRIL 2, 2020 • NO. 5

NYDFS Extends Part 500 Cybersecurity Regulation Certificate of Compliance Filing Deadline

Recognizing the challenges that regulated entities now face in light of the growing COVID-19 public health emergency, and to assist impacted regulated entities in meeting their regulations under the New York Banking Law and Financial Services Law, the New York Department of Financial Services ("NYDFS") recently issued its "Order Granting Temporary Relief to COVID-19 Affected Regulated Entities and Persons," which, among other things, extends the NYDFS Part 500 Cybersecurity Regulation Certificate of Compliance filing deadline from April 15 to June 1, 2020. The Order does not, however, modify regulated entities' obligation under the Cybersecurity Regulation to notify the NYDFS of a cybersecurity event. While the Order provides some breathing room in terms of the applicable compliance deadline for Certificates of Compliance, regulated entities that have not already finalized their Certificates should take immediate action now to ensure they are able to meet the extended June filing deadline.

The NYDFS Part 500 Cybersecurity Regulation

In March 2017, the NYDFS promulgated a new, sweeping cybersecurity regulation geared toward protecting customer information and safeguarding the information technology systems of regulated entities. Generally speaking, the Cybersecurity Regulation requires regulated entities to conduct a detailed risk assessment to assess the organization's cybersecurity risks and the effectiveness of its cyber defenses, and then design a cybersecurity program guided by the risk assessment that protects the confidentiality, integrity, and availability of the entity's networks and systems. In doing so, regulated entities must satisfy specified regulatory minimum standards that have been implemented by the NYDFS to minimize the risk of cyber breach events.

A core component of the Cybersecurity Regulation requires regulated entities to submit, on a yearly basis, a Certificate of Compliance covering the prior calendar year which certifies that the entity has complied with the Cybersecurity Regulation. In addition, regulated entities must also maintain records supporting their Certification for five years. Regulated entities that are exempt from the Cybersecurity Regulation are required to provide notice to the NYDFS of their exempt status.

Penalties for violations of the Cybersecurity Regulation are authorized under the New York Banking Law of up to: (1) $2,500 per day for continuing violations; (2) $15,000 per day for violations that are reckless, or which constitute an unsound practice or pattern of conduct; and (3) $75,000 per day for knowing and willful violations.

The NYDFS's COVID-19 Temporary Relief Order

On March 12, 2020, the NYDFS issued its Order Granting Temporary Relief to COVID-19 Regulated Entities and Persons, which, in addition to providing other various forms of relief, extends the Certificate of Compliance filing deadline for a period of 45 days—from April 15 to June 1, 2020—for entities that are unable to meet the original deadline due to issues arising from COVID-19. Thus, all regulated entities that are not fully exempt from the Cybersecurity Regulation are required to submit a Certification of Compliance no later than June 1, 2020, attesting to their compliance for the 2019 calendar year.

In addition, the Order also extends additional filing deadlines and relaxes certain requirements for temporary relocations, branch closings, and remote board/trustee/committee meetings. At the same time, the Order also emphasizes regulated entities' ongoing obligations to maintain appropriate data security and cybersecurity safeguards and controls for all remote workers and to provide the NYDFS with "prompt" notice of any relocations or branch shutdowns. The regulatory relief afforded by the Order will remain in effect until further modified by the DFS.

Compliance Steps

The Certificate of Compliance filing deadline extension applies to "regulated entities and persons unable to meet filing deadlines due to the outbreak of COVID-19." The broad language in this context indicates that the extension should be applicable to any regulated entities that are unable to satisfy the original April 15 deadline due to a wide range of issues relating to COVID-19, including staffing or personnel limitations, difficulties in obtaining information needed to complete the certification, and technology-related issues that have arisen as a result of the current public health emergency. With that said, in the event a regulated entity files its Certificate of Compliance after April 15, it should ensure that it thoroughly documents all relevant circumstances and/or challenges relating to COVID-19 that required the entity to rely on the extended filing deadline.

Those regulated entities that are fully exempt from the Cybersecurity Regulation and have already filed a previous notice of exemption do not have to submit a new notice at this time. However, if there has been any change in an entity's exemption status, that entity should amend or terminate its exemption and notify the NYDFS of any such change in status.

Regulated entities can file their Certificates of Compliance digitally using the NYDFS Cybersecurity Portal, available here.

Conclusion

The NYDFS has made clear that ensuring compliance with the Cybersecurity Regulation will be a priority for the department, and recently created a new Cybersecurity Division for that specific purpose. Together, the NYDFS has clearly signaled its intent to vigorously enforce compliance with the law. Combined with the NYDFS's reputation as an aggressive regulator, the cost of failing to comply with the Cybersecurity Regulation will be significant. Regulated entities should not assume that non-compliance will be excused simply because of the current public health emergency. This is especially so for the Certificate of Compliance component of the law, which the NYDFS has characterized as a "critical governance pillar for the cybersecurity program of all DFS regulated entities."

As part of its COVID-19 Task Force, Blank Rome's Cybersecurity & Data Privacy professionals can assist with providing key counseling and guidance with respect to any issues or concerns relating to the Certificate of Compliance component of NYDFS Cybersecurity Regulation or any other aspect of New York's sweeping cybersecurity law. And if you find yourself the victim of a cybersecurity event, Blank Rome's data breach incident response team is available 24/7, and can provide immediate assistance with rapid incident response and crisis management following a data breach event.

For additional information, please contact:

Jennifer J. Daniels, Pittsburgh Office
Partner, Cybersecurity & Data Privacy
412.932.2754 | daniels@blankrome.com

David J. Oberly, Cincinnati Office
Associate, Cybersecurity & Data Privacy,
Privacy Class Action Defense
513.362.8711 | doberly@blankrome.com